CLAIMS

What is claimed is:

[6,055,636]

1. A method comprising:

reading distinguished name data from a signed certificate received from a certificate authority; and 5,45-50

searching a data structure to identify a certificate signing request associated with the signed certificate, 3,29-31 the identified certificate signing request corresponding to the read distinguished name data. 2,38-39
3,49-54

2. The method of claim 1, further comprising identifying a key pair associated with the signed certificate. 2,49-54

3. The method of claim 1, the read distinguished name data comprising all of the distinguished name data contained in the signed certificate. 5,18-22

4. The method of claim 1, the identified certificate signing request corresponding to a portion of the read distinguished name data. 5,18-22

5. The method of claim 1, further comprising importing the signed certificate to a server associated with the identified certificate signing request.

6. The method of claim 5, wherein the signed certificate is imported to a device that performs SSL processing on behalf of the server.

7. The method of claim 1, further comprising identifying at least two certificate signing requests associated with the signed certificate. 3, 31-45

8. A method comprising:

providing a mapping table including distinguished name data for each of a plurality of certificate signing requests;

extracting distinguished name data from a signed certificate received from a certificate authority; and

*comparing the extracted distinguished name data with the mapping table data to identify a certificate signing request associated with the signed certificate from the plurality of certificate signing requests.

9. The method of claim 8, the mapping table including at least a common name for each of the plurality of certificate signing requests.

10. The method of claim 8, the extracted distinguished name data comprising all of the distinguished name data contained in the signed certificate.

11. The method of claim 8, the extracted distinguished name data comprising a common name.

0 12. The method of claim 8, further comprising comparing a portion of the extracted distinguished name data with a portion of the distinguished name data of each certificate signing request contained in the mapping table to identify the certificate signing request associated with the signed certificate.

6 13. The method of claim 12, the portion of the extracted distinguished name data comprising a common name.

14. The method of claim 8, further comprising:

comparing the extracted distinguished name data with the mapping table data to identify at least two certificate signing requests from the plurality of certificate signing requests; and

determining which of the at least two certificate signing requests is associated with the signed certificate.

15. The method of claim 14, further comprising performing a second search of the mapping table data to determine which of the at least two certificate signing requests is associated with the signed certificate.

16. The method of claim 8, further comprising importing the signed certificate to a server associated with the identified certificate signing request.

17. The method of claim 16, wherein the signed certificate is imported to a device that performs SSL processing on behalf of the server.

18. The method of claim 8, further comprising identifying at least two certificate signing requests associated with the signed certificate.

19. A method comprising:

generating a certificate signing request, the certificate signing request including distinguished name data;

storing the distinguished name data in a mapping table;

transmitting the certificate signing request to a certificate authority; 1, 64-65

receiving a signed certificate from the certificate authority, the signed certificate including distinguished name data; 1, 58-60

extracting the distinguished name data from the signed certificate; and 2, 45-47

comparing the extracted distinguished name data with the stored distinguished name data contained in the mapping table to identify the certificate signing request.

20. The method of claim 19, the stored distinguished name data comprising all of the distinguished name data contained in the certificate signing request. 3, 31-45

21. The method of claim 19, the stored distinguished name data comprising a common name.

22. The method of claim 19, further comprising comparing a portion of the extracted distinguished name data with a portion of the stored distinguished name data.

23. The method of claim 19, further comprising comparing a common name contained in the extracted distinguished name data with a common name contained in the stored distinguished name data.

24. The method of claim 19, the extracted distinguished name data comprising all of the distinguished name data contained in the signed certificate.

25. The method of claim 19, the extracted distinguished name data comprising a common name.

26. The method of claim 19, further comprising:
generating a key pair associated with the certificate signing request; and
identifying the key pair when comparing the extracted distinguished name data with the stored distinguished name data.

27. The method of claim 19, further comprising importing the signed certificate to a server associated with the certificate signing request.

28. The method of claim 19, further comprising importing the signed certificate to an SSL processing device.

112 2nd

29. A system comprising: (103)

a memory coupled with a bus, the memory having a mapping table resident thereon; and

a processing device coupled with the bus, the processing device to

read distinguished name data from a signed certificate received from a certificate authority, and

search the mapping table to identify a certificate signing request associated with the signed certificate, the identified certificate signing request corresponding to the read distinguished name data.

30. The system of claim 29, the processing device to identify a key pair associated with the signed certificate.

31. The system of claim 29, the read distinguished name data comprising all of the distinguished name data contained in the signed certificate.

32. The system of claim 29, the identified certificate signing request corresponding to a portion of the read distinguished name data.

33. The system of claim 29, the memory comprising a non-volatile data storage device.

34. The system of claim 29, wherein a plurality of servers are coupled with the bus, the processing device to download the signed certificate to a selected server of the plurality of servers, the selected server associated with the identified certificate signing request.

35. The system of claim 29, wherein an SSL processing device is coupled with the bus, the processing device to download the signed certificate to the SSL processing device.

36. An article of manufacture comprising:

a machine accessible medium providing content that, when accessed by a machine, causes the machine to

read distinguished name data from a signed certificate received from a certificate authority; and

search a data structure to identify a certificate signing request associated with the signed certificate, the identified certificate signing request corresponding to the read distinguished name data.

37. The article of manufacture of claim 36, wherein the content, when accessed, further causes the machine to identify a key pair associated with the signed certificate.

38. The article of manufacture of claim 36, the read distinguished name data comprising all of the distinguished name data contained in the signed certificate.

39. The article of manufacture of claim 36, the identified certificate signing request corresponding to a portion of the read distinguished name data.

40. The article of manufacture of claim 36, wherein the content, when accessed, further causes the machine to import the signed certificate to a server associated with the identified certificate signing request.

41. The article of manufacture of claim 40, wherein the content, when accessed, further causes the machine to import the signed certificate to a device that performs SSL processing on behalf of the server.

42. The article of manufacture of claim 36, wherein the content, when accessed, further causes the machine to identify at least two certificate signing requests associated with the signed certificate.

43. An article of manufacture comprising:

a machine accessible medium providing content that, when accessed by a machine, causes the machine to

provide a mapping table including distinguished name data for each of a plurality of certificate signing requests;

extract distinguished name data from a signed certificate received from a certificate authority; and

compare the extracted distinguished name data with the mapping table data to identify a certificate signing request associated with the signed certificate from the plurality of certificate signing requests.

44. The article of manufacture of claim 43, the mapping table including at least a common name for each of the plurality of certificate signing requests.

45. The article of manufacture of claim 43, the extracted distinguished name data comprising all of the distinguished name data contained in the signed certificate.

46. The article of manufacture of claim 43, the extracted distinguished name data comprising a common name.

47. The article of manufacture of claim 43, wherein the content, when accessed, further causes the machine to compare a portion of the extracted distinguished name data with a portion of the distinguished name data of each certificate signing request contained in the mapping table to identify the certificate signing request associated with the signed certificate.

48. The article of manufacture of claim 47, the portion of the extracted distinguished name data comprising a common name.

49. The article of manufacture of claim 43, wherein the content, when accessed, further causes the machine to:

compare the extracted distinguished name data with the mapping table data to identify at least two certificate signing requests from the plurality of certificate signing requests; and

determine which of the at least two certificate signing requests is associated with the signed certificate.

50. The article of manufacture of claim 49, wherein the content, when accessed, further causes the machine to perform a second search of the mapping table data to determine which of the at least two certificate signing requests is associated with the signed certificate.

51. The article of manufacture of claim 43, wherein the content, when accessed, further causes the machine to import the signed certificate to a server associated with the identified certificate signing request.

52. The article of manufacture of claim 51, wherein the content, when accessed, further causes the machine to import the signed certificate to a device that performs SSL processing on behalf of the server.

53. The method of claim 43, wherein the content, when accessed, further causes the machine to identify at least two certificate signing requests associated with the signed certificate.

54. An article of manúfacture comprising:

10?

a machine accessible medium providing content that, when accessed by a machine, causes the machine to

x generate a certificate signing request, the certificate signing request including distinguished name data;

[store the distinguished name data in a mapping table;]

transmit the certificate signing request to a certificate authority;

receive a signed certificate from the certificate authority, the signed certificate including distinguished name data;

extract the distinguished name data from the signed certificate; and

compare the extracted distinguished name data with the stored distinguished name data contained in the mapping table to identify the certificate signing request.

55. The article of manufacture of claim 54, the stored distinguished name data comprising all of the distinguished name data contained in the certificate signing request.

56. The article of manufacture of claim 54, the stored distinguished name data comprising a common name.

57. The article of manufacture of claim 54, wherein the content, when accessed, further causes the machine to compare a portion of the extracted distinguished name data with a portion of the stored distinguished name data.

58. The article of manufacture of claim 54, wherein the content, when accessed, further causes the machine to compare a common name contained in the extracted distinguished name data with a common name contained in the stored distinguished name data.

59. The article of manufacture of claim 54, the extracted distinguished name data comprising all of the distinguished name data contained in the signed certificate.

60. The article of manufacture of claim 54, the extracted distinguished name data comprising a common name.

61. The article of manufacture of claim 54, wherein the content, when accessed, further causes the machine to:

generate a key pair associated with the certificate signing request; and

identify the key pair when comparing the extracted distinguished name data with the stored distinguished name data.

62. The article of manufacture of claim 54, wherein the content, when accessed, further causes the machine to import the signed certificate to a server associated with the certificate signing request.

63. The article of manufacture of claim 54, wherein the content, when accessed, further causes the machine to import the signed certificate to an SSL processing device.